UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TENNESSEE AT GREENEVILLE

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 2:16-CR-103**
	)	**JUDGES GREER/CORKER**
MATTHEW HARRISON MARTLAND	)	

POST-HEARING BRIEF IN SUPPORT OF MOTION TO SUPPRESS

The defendant, MATTHEW HARRISON MARTLAND, by and through counsel pursuant to the Fourth Amendment to the United States Constitution; *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); and other authorities cited herein, respectfully submits this supplemental brief following the December 4, 2017 hearing on Mr. Martland's motion to suppress [Doc. 82]. *See* Order [Doc. 137] (inviting supplemental briefing).

I. INTRODUCTION

Through three warrantless searches, the government has seized over 100 gigabytes of information from Wellco Enterprises, Inc., and Original Footwear, Inc., the company that purchased Wellco out of bankruptcy in 2014. Included in the warrantlessly seized information are Mr. Martland's business and personal email communications and his business documents. Mr. Martland moved to suppress this warrantlessly seized information, and this Court held an evidentiary hearing on the suppression issues on December 4, 2017.

The evidence at the hearing showed that Mr. Martland had a subjective expectation of privacy in the warrantlessly seized communications. The Sixth Circuit has recognized that this expectation is objectively reasonable, and held in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), that individuals have a reasonable expectation of privacy in their personal and business communications stored by a third party that had right of access. Mr. Martland enjoys an even

greater expectation of privacy in his emails which were stored on the private server of a private company and accessible only by Mr. Martland via his smart phone and his computer.

The government has argued that Mr. Martland could have no expectation of privacy in this information because Wellco maintained a corporate right of access policy with respect to employee emails. The applicability of these policies to Mr. Martland is unclear, but even assuming they did apply, the government's argument misses the point – Wellco's ability to access Mr. Martland's company email account did not diminish his expectation that the emails would remain private as to the general public and the government. In practice, Wellco's ability to access employee emails was restricted, company access of employee emails was infrequent and limited to job performance issues, and Mr. Martland's communications were not accessed or reviewed by Wellco.

Mr. Martland also has standing to contest the warrantless seizure of additional business documents the government may seek to attribute to him due to his managerial position at Wellco, the fact that he was a target of the government's investigation, and that he took steps to protect his documents, like maintaining secure log-in credentials on his workplace computer and the company domain/file server.

The government has the burden of proving a valid exception to the warrant requirement, and it has not done so in this case. Accordingly, Mr. Martland's warrantlessly seized communications and records must be suppressed.

II. DECEMBER 4, 2017 EVIDENTIARY HEARING

At the hearing, the government presented testimony of Special Agent John Witsell, the lead Homeland Security Investigations agent in the case, (Tr., p. 8:10-15)[1] and David Mason, the former

[1] Citations are made to the transcript of the December 4, 2017 evidentiary hearing in the following format: (Tr., p. [page number]: [line number]), because the transcript has not been published electronically on the record yet. *See* Notice of Filing of Official Transcript [Doc. 143].

Senior Information Technology ("IT") Administrator for Tactical Holdings Operations, Inc., the parent company for Wellco Enterprises, Inc. (*See* Tr., p. 13:20-14:11; 136:17-137:3). Mr. Martland testified pursuant to *Simmons v. United States*, 390 U.S. 377, 394 (1968) (holding "when a defendant testifies in support of a motion to suppress evidence on Fourth Amendment grounds, his testimony may not thereafter be admitted against him on the issue of guilt[.]"). (*See* Tr., p. 230:23-231:7). The other defendants did not testify.

A. The administration of Wellco's file and email servers.

Wellco locally housed two servers at its manufacturing facility in Morristown, Tennessee, (*id*. at p. 148:11-14). One server was a Windows file server with a domain controller – software that enabled creation of log-in credentials so that individual users' workstations could access the files stored on the server. (*Id*. at p. 148:15-149:3). The other server, an AS400 system, stored Tactical Holdings' Enterprise Resource Planning software, which contained the company's inventory system and business functions. (*Id*. at p. 149:14-150:8).

Tactical Holdings used a Microsoft Exchange server to house individual user email, calendaring, contacts, and related information accessible to users via Microsoft Outlook on a workstation or via a mobile device, such as an iPhone. (*Id*. at p. 153:20-23; 156:23-6). An Exchange server is a piece of email software that resides on a Windows server. (*Id*. at p. 157:2-6). The emails sent and received through Outlook or an iPhone resided both on the Exchange server and locally on an individual user's computer or device. (*Id*. at p. 225:9-11). Users had control over how their emails were organized and saved; users could create folders and subfolders within Outlook or their mobile device to store their emails – these folders were replicated on the Exchange server, but users could opt to store some emails in those folders only on their local machine. (*Id*. at p. 154:9-155:5). Users could also use the calendar function in Outlook to store calendar entries,

which would be saved and stored to the Exchange server. (*Id*. at p. 154:12-17). Users could store their contacts within Outlook and their mobile device, and the contacts would be replicated and stored on the Exchange server. (*Id*. at p. 156:2-13).

At Wellco, users had different credentials for the domain/file server and for the Exchange server because the Exchange server did not reside at the Wellco facility and was not administered by Wellco. (*Id*. at p. 158:10-159:2). The Wellco Exchange server was managed by a company called MicroCerv in Alcoa, Tennessee; Byron Doss was primary point of contact for Wellco's IT department, including Mr. Mason. (*Id*. at p. 159:3-21). Mr. Doss also externally maintained the the internal network for Tactical Holdings. (*Id*. at 165:19-21).

Anything concerning the Exchange server had to be done through Mr. Doss because no Tactical Holdings employee, including Mr. Mason, could physically or virtually access the server. (*Id*. at p. 164:11-13; p. 166:22-167:9). The Exchange server was housed by Mr. Doss in downtown Knoxville at Digital Crossings, a secure facility with security conforming with heightened data center security standards, and only Mr. Doss had the credentials necessary to physically access the email server. (*Id*. at p. 160:1-12; p. 161:14-17; p. 161:14-162:22; p. 162:17-163:12). Similarly, no Tactical Holdings employee had the administrative privileges necessary to access the electronic communications stored on the Exchange server. (*See id*. at p. 164:1-4).

Wellco users enjoyed a great deal of control over their email accounts. In most cases, users contacted Mr. Doss directly to set up their log-in credentials, meaning that only Mr. Doss and the user would know the password for that person's email, calendaring, contacts and other information stored on the Exchange server. (*See id*. at p. 224:3-20). In any situation where a user needed his or her credentials changed for their email account, it was necessary for Mr. Doss to handle it. (*Id*. at p. 143:18-25; 167:8-9). Wellco users could permanently delete emails from the email server when

they deleted them from their individual accounts. As a matter of course, emails were not saved on the file server stored in Morristown, and were only stored on the Exchange server. (*Id*. at p. 225:7-11). When a user deleted an email from their work account, the email was not only deleted from their computer, but also from the Exchange server. (*Id*. at p. 225:12-226:5). Users could also save emails to their local workstations, where they would only be accessible by that user via their domain log-in credentials. (*Id*. at p. 152:11-15). Mr. Mason stated that even he could not easily obtain a user's domain server credentials, even though that was the on-site server administered by Mr. Mason. (*Id*. at p. 168:25-169:3).

B. Mr. Martland's expectation of privacy in his emails and business documents.

Mr. Martland worked at Wellco as the Director of Distribution and Logistics from January 2010 to July 2012, and managed five warehouse employees and two administrative assistants. (*Id*. at p. 233:11-18; p. 234:4-7). Mr. Martland shared an office in Wellco's warehouse with his two administrative assistants. (*Id*. at p. 234:16-17). In his office, Mr. Martland had a desktop computer that was accessible only using log-in credentials unique to Mr. Martland's account and specific to his particular workstation. (*Id*. at p. 151:24-152:2; p. 234:21-235:6). This set of log-in credentials was controlled by the domain/file server that physically resided at Wellco and administered by Mr. Mason. (*Id*. at p. 151:12-15). Mr. Martland could access and save files locally on his computer, and those locally saved files could not be accessed by anyone other than Mr. Martland unless they knew the username and password for his workstation. (*Id*. at p. 152:11-15). Mr. Martland could also access and save files to a shared drive that was on the domain/file server. (*Id*. at p. 152:7-10; p. 191:12-24). Other users' accounts and workstations were set-up in a similar manner. (*Id*. at p. 152:18-20).

Mr. Martland had Microsoft Outlook on his desktop computer, (*id*. at p. 156:14-17), and was also able to access his emails, contacts, and calendar using an iPhone provided to him by the company. (*Id*. at p. 221:25-222:9). Like all users, Mr. Martland's log-in credentials for the Exchange server were created by Mr. Doss. (*Id*. at p. 222:6-9). Mr. Martland's account stored his emails, calendar entries, and contacts on the Exchange server and locally on his workstation, and Mr. Martland could access and make changes to this information on the Exchange server. (*Id*. at p. 157:13-158:9; p. 164:14-25),

Mr. Martland used his Wellco Exchange/Outlook account for all aspects of his business and personal life, to include the most intimate details of his life. Mr. Martland's company email account was the primary email he used to send and receive both personal and business communications via his mobile device and his workstation in his office. (*Id*. at p. 235:22-25). For example, Mr. Martland used his company email to communicate with his personal friends, his wife (who was his girlfriend at the time), and his mother, and would coordinate family trips or dinners via email. (*Id*. at p. 235:10-18; 307:18-308:13). Mr. Martland also used his Outlook calendar to store his business and personal calendar entries, and stored anything from business meetings to "doctor's appointments, dentist's appointments, dinners that we may have with my in-laws…my girlfriend at the time or with my mother." (*Id*. at p. 236:12-22). He also kept his personal contacts in Outlook, and when he began using a work-issued iPhone, all of his contacts automatically synced to his Wellco Exchange account so that entries in Outlook on his workstation were replicated on his iPhone. (*Id*. at p. 237:15-238:10).

Mr. Martland's Outlook/Exchange account was password protected. (*Id*. at p. 239:7-11), and he testified that he never shared his username and password with anyone at Wellco. (*Id*. at p. 239:7-11; p. 242:8-10). Mr. Martland said that he knew his desktop computer and iPhone were

connected to an Exchange server, and that the Exchange server was stored off-site. (Tr., p. 238:13-25). Mr. Martland said that he believed that Wellco's Exchange server was more secure, and that his emails were more private, than if he had an email account with a public internet company such as Google or Yahoo. (*Id*. at p. 262:13-263:14).

Mr. Martland testified that he did not expect Wellco to gain access to and monitor his emails, and that he expected everything he was doing to be private. (Tr., p. 240:9-12). Mr. Martland believed he could freely use his company email account for business and personal use. (*Id*. at p. 242:1-7). Before he was hired by Wellco, he was close to the Ferguson family, including Lee Ferguson, the CEO of the company, and they would send him personal communications from company email accounts, (*id.* at p. 241:19-22), and while he was a Wellco employee, he continued to use his company email to engage in personal, non-business communications with Lee Ferguson and others in the company – further validating his expectation that he could use his company email account for personal use. (*Id*. at p. 264:4-13).

Mr. Martland testified that because he believed he could freely use his account for personal communications, he would not have expected his supervisor to request access to his Outlook/Exchange account information. (*See id*. at p. 241:7-25). Mr. Martland never asked IT to allow him to review or monitor the Outlook/Exchange account of the employees he supervised, and he was not told he had the opportunity to look at his employee's emails. (*Id*. at p. 240:3-8; 241:23-25). Mr. Martland believed, because of his managerial role, that he had more autonomy than an associate employee and a greater expectation of privacy in his communications. (*Id.* at p. 259:22-260:3). Mr. Mason testified that he was never asked to monitor or gain access to Mr. Martland's emails, and he never did so. (*Id*. at p. 196:25-197:3).

Mr. Martland left Wellco in July of 2012, after accepting a job from his former employer, C.H. Robinson. (*Id*. at p. 244:23-245:9). It was Mr. Martland's understanding that the three-week notice period before he left Wellco was to make sure that any relevant emails or documents on his company email account were passed along to his administrative assistants, as he thought his Exhange account, and all the information linked to it, would be deleted once he was no longer an employee. (*Id*. at p. 288:8-25). Mr. Martland said this occurred with his University of Tennessee student email address, which was shut-off once he was no longer a student. (*Id*. at p. 318:8-12).

C. The government's warrantless seizures from Wellco's servers.

Agent Witsell began investigating Wellco in "early 2012", after the Office of Foreign Asset Controls ("OFAC") became aware that Wellco shipped boots to a sanctioned diamond mine in Africa. (*Id*. at p. 8:18-19-9:4; p. 74:16-21). After the OFAC investigation concluded, Agent Witsell continued a criminal investigation into Wellco after learning that two shipments of Wellco merchandise had been detained in Savannah, Georgia. (*Id*. at p. 9:14-21). During his investigation, he regularly conferred with the U.S. Attorney's Office for the Eastern District of Tennessee. (*See id.* at p. 126:6-16; p. 131:13-132:3). By February of 2013, Agent Witsell was openly performing a criminal investigation into Wellco. (*See* Exhibit and Witness List [Doc. 135], Exhibit 13, p. 2; Tr., p. 73:13-75:3; p. 76:3-8 (Agent Witsell told Neil Streeter during an interview on February 21, 2013, that he "was not continuing the investigation concerning the OFAC violations, but [was] in fact investigating criminal violations that had been discovered.")).

To further his investigation into Wellco, Agent Witsell issued a Department of Homeland Security ("DHS") administrative summons to Wellco on May 20, 2013. (Tr. p. 9:22-10:25; *see* Exhibit and Witness List [Doc. 135], Exhibit 1). The DHS summons "required" Wellco to produce a wide range of information spanning from January 1, 2008 to December 31, 2012, including "any

and all documents that support the summoned information in whatever format they may be stored (printed documents; emails; notes; phone messages; etc.)". (Exhibit and Witness List [Doc. 135], Exhibit 1, p. 3). Agent Witsell acknowledged that the summons was not a "request" for document production and that Wellco's compliance was commanded. (*See* Tr., p. 76:24-77:5).

Wellco's corporate counsel worked "hand and glove" with the government to respond to the summons. (*Id*. at p. 11:17-19; p. 78:21-24). In August 2013, after Wellco had already produced documents in response to the summons, Agent Witsell emailed corporate counsel and expanded the parameters of the required production to specifically include emails and business documents from Mr. Martland. (*Id*. at p. 11:23-12:10; *see also* Exhibit and Witness List [Doc. 135], Exhibit 2). In response to the DHS summons and emails from Agent Witsell expanding the terms of the search, Wellco produced approximately 100,000 documents to the government, including Mr. Martland's emails and business records. (Tr., p. 16:8-11; p. 176:12-15).

Despite Wellco's voluminous document production, the government returned to the well and warrantlessly obtained additional Wellco documents multiple times. In late 2015, Agent Witsell went to the Original Footwear facility with the intention of physically taking the entire file server containing Wellco's documents. (*Id*. at p. 83:14-20). After realizing that removing the file server was physically impossible due to its size, Agent Witsell left and another Department of Homeland Security agent returned later and digitally copied large portions of the Wellco file server. (*Id*. at p. 83:21-84:2; p. 85:3-10).

During this collection, the government was given nearly unlimited access to the materials stored on Wellco's file server. Mr. Mason assisted Dominic Magliara, the DHS agent working with Agent Witsell, with accessing the server. (*Id.* at p. 186:19-22; p. 187-18-20). Agent Magliara brought an external hard drive to the facility and asked Mr. Mason how to find documents relating

to certain key words. (*Id*. at p. 188:3-11). Mr. Mason provided Agent Magliara with a set of log-in credentials for Wellco's file server and showed him how to access the server and copy documents to the external hard-drive. (*Id*. at p. 188:12-189:1; p. 189:15-190:1). Mr. Mason sat with Agent Magliara the first few times while he copied documents, but after that, Mr. Mason left and Agent Magliara continued copying any files he wanted. (*Id*. at p. 193:3-11). Mr. Mason said that he didn't know how many files Agent Magliara took, but that it was a large amount of information. (*Id*. at p. 192:18-193:11).

After Mr. Martland was charged criminally, the government continued to warrantlessly seize information. On November 17, 2017, and in anticipation of the evidentiary hearing on Mr. Martland's motion to suppress, Agent Witsell interviewed Mr. Mason and asked him to obtain documents containing Wellco privacy and monitoring policies. (*Id*. at p. 17:14-17; p. 179:5-9). Mr. Mason still works as a contractor for Original Footwear, and had remote access via a VPN (virtual private network) to the Wellco files stored on Original Footwear's server. (*Id*. at p. 20:10-13). Mr. Mason provided Agent Witsell with "quite a few" documents from the Original Footwear server – he did not read the contents of the documents he produced, but retrieved documents just based on file names that "sort of matched" Agent Witsell's interview topics. (*Id*. at p. 180:20-181:2; p. 182:4-10; p. 183:139-184:7).

Mr. Mason was involved with each of the government's warrantless seizures, and testified that it was his understanding that on each occasion he provided documents to the government, he was assisting the company in complying with some kind of legal directive. (*Id*. at p. 212:6-17). In 2013, Lee Ferguson informed Mr. Mason that Wellco was working with the government, and that he should provide help where needed during that process. (*Id*. at p. 227:8-25). Mr. Mason further testified that sometime before he was interviewed by Agent Witsell in November 2017, he received

an email from Mr. Cole instructing him to comply with "something", though he said he wasn't sure whether it was the subpoena or a summons. (Tr., p. 212:10-13).

D. Wellco's alleged privacy and monitoring policies.

Among the documents that Agent Witsell seized during the November 17, 2017 interview were several electronic word processor versions of draft documents and draft employee handbooks. (*See id*. at p. 17:23-25; p. 19:20-24). These documents were obtained by the government in editable electronic formats, and the government could not establish that they represented actual, final versions of policies that were distributed to employees, other than a .pdf file of an employment contract that appeared to have been signed by Lee Ferguson and scanned and saved to the Wellco file server. (*Id*. at p. 92:15-94:2; 183:19-184:7).

It is further unclear whether some of the policies introduced by the government would have applied to Mr. Martland because the draft 2011 associate handbook (the only handbook relevant to Mr. Martland's period of employment with Wellco) contains numerous distinctions between associate employees and managerial or supervisory employees. (*See e.g.*, Exhibit and Witness List [Doc. 135], Exhibit 6, p. 5 (instructing associates to discuss concerns about workplace issues with a manager)). At any rate, the policies introduced at the hearing are vague and confusing. For example, the 2011 handbook prohibited employees from storing company files on personal computers but in a separate section on the same page, instructed employees to return company documents stored on personal computers at the end of their employment. (*Id.* at p. 30; *see also* Exhibit and Witness List [Doc. 135], Exhibit 8, p. 13; Tr., p. 104:19-106:17 (for example, Lee Ferguson's employment letter contained a provision certifying that he'd returned company property, despite the fact that he'd not begun his employment yet)).

Attempting to clarify the issue, the government introduced an unsigned copy of Mr. Martland's employment agreement which stated that he would be taking a "salary exempt position." (Tr., p. 53:1-4; Exhibit and Witness List [Doc. 135], Exhibit 10, p. 1). The 2011 Associate Handbook states: "For the administration of pay and benefits Associates are further classified as follows: 1. Hourly – Non-exempt 2. Administrative Hourly – Non-exempt 3. Salary – Exempt." (Exhibit and Witness List [Doc. 135], Exhibit 6, p. 10). The government noted that the Associate Handbook refers to itself as an "employee handbook" to evidence its applicability to Mr. Martland. (*See* Tr. at p. 30:5-13).

Mr. Martland agreed that he was a "salary-exempt" employee, but because of these distinctions, he did not think the policies in the handbook applied to his managerial position. (*Id.* at p. 244:17-22; p. 271:14-272:12; p. 297:9-13). Mr. Martland said that when he received his employment offer letter, he never received a document explaining what a "salary-exempt" position was, and that he did not receive an employee handbook until 2011, over a year after his employment with Wellco began. (*Id.* at p. 314:7-17). He received a handbook similar to Exhibit 6, but he was unsure whether Exhibit 6 was representative of the handbook he actually received. (*Id.* at p. 264:14-265:4).

If they were applicable to Mr. Martland, the policies contained in the draft associate handbook established that Wellco would access or monitor employee emails on a limited basis for work-related reasons – not that Wellco would disclose employee emails to the government or general public. For example, the 2011 associate employee handbook contained a statement that:

> Associates should have NO expectation of privacy when using company systems. The voice, electronic mail, and internet access systems and all voice recordings, mail, and activities generated on these systems are Company property and should be used for work-related and business purposes only.... The Company will monitor voice recordings, E-mail messages, Internet access, and systems on a periodic and/or random basis and as otherwise deemed appropriate.

(Exhibit and Witness List [Doc. 135], Exhibit 6, p. 33; *see also id.* at p. 20).

The evidence regarding Wellco's actual business practices revealed that Wellco's corporate right of access was limited and infrequently exercised. The government introduced evidence of only a single instance of a Wellco employee's emails being monitored by the company, and those emails were monitored for work-related reasons. Wellco began monitoring the company email account of Tyler Morley, the former Director of Military Sales for Wellco after repeated job performance issues, including stealing company documents and using email malfunctions as excuses for his failing job performance. (*See* Exhibit and Witness List [Doc. 135], Exhibit 12, 12/05/2011 entry; *see also* Tr., p. 63:24-64:19). These issues persisted for nearly a year and a half before CEO Lee Ferguson eventually authorized monitoring of his emails and mobile device. (*See* Exhibit and Witness List [Doc. 135], Exhibit 12, 7/13/11 entry; 9/22/11 entry; 11/11/2011 entry).

Mr. Mason explained that Kathy Smith, the Wellco Director of Human Resources, called him into her office and asked him to find out where Mr. Morley was, and "find a way to see if he's ex-filtrating data." (Tr. p, 142:5-7). Mr. Mason told Ms. Smith that, "[r]eally the only thing we can do [to monitor Mr. Morley's emails] is reset his password." (*Id*. at p. 168:22-25). Mr. Mason said that was "really the only choice", since he didn't know Mr. Morley's credentials, and didn't have a way to figure out what Mr. Morley's credentials were. (*Id*. at p. 168:25-169:3). Mr. Mason said Mr. Morley's emails were monitored because there were suspicions about Mr. Morley's work performance and that he was improperly taking company information. (*Id*. at p. 197:4-12).

To reset Mr. Morley's password, it was necessary to involve Mr. Doss at MicroCerv. (*Id*. at p. p. 143:21-25 ("We didn't have credentials, necessary credentials to do it. So we would always reach out to [Byron Doss] for things like that.")). After Mr. Doss changed Mr. Morley's password, Mr. Morley called because his email wasn't working, and Mr. Mason gave him the new password

that Wellco knew; then Wellco was able to log-in and view Mr. Morley's company email account to examine his job performance issues. (Tr., p. 8-16; p. 172:1-24).

One Wellco draft policy was clear – that employees were entitled to "safeguards provided by law" in the event of a government investigation. (*See* Exhibit and Witness List [Doc. 135], Exhibit 7, p. 9). Agent Witsell acknowledged that "safeguards provided by law" is a broad term, and that the policy assured employees that they would receive a wide range of legal protections in the event of a government investigation. (*See* Tr., p. 103:5-18). Agent Witsell also admitted that representation of counsel and a search warrant are legal safeguards employees would be entitled to during a government investigation. (*Id*. at p. 103:5-24).

III. MR. MARTLAND HAS STANDING TO CONTEST THE WARRANTLESS SEIZURE OF WELLCO DOCUMENTS.

"[C]apacity to claim the protection of the Fourth Amendment depends not upon a property right in the invaded place, but upon whether the area was one in which there was a reasonable expectation of freedom from government intrusion." *Mancusi v. Deforte*, 392 U.S. 364, 368 (1968); *see also United States v. Gooch*, 499 F.3d 596, 600 (6th Cir. 2007). Whether a person has a reasonable expectation of privacy in a certain item or area is a two-part inquiry: "first, has the [target of the investigation] manifested a subjective expectation of privacy in the object of the challenged search: Second, is society willing to recognize that expectation as reasonable?" *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (citing *Ciraolo*, 476 U.S. at 211). A warrantless search or seizure into a constitutionally protected area "'is per se unreasonable…subject to only a few specifically and well-delineated exceptions.'" *United States v. Doxey*, 833 F.3d 692, 703 (6th Cir. 2017) (citing *Sneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)). The government has the burden of proving that a valid

exception to the warrant requirement applied. *United States v. Kinney*, 638 F.2d 941, 943 (6th Cir. 1981) (citing *Vale v. Louisiana*, 399 U.S. 30 (1970)).

A. Mr. Martland established his subjective expectation of privacy.

Mr. Martland testified that he used his company Outlook/Exchange account for all manner of business and personal purposes. Mr. Martland knew that other members of the company, including Lee Ferguson, the CEO, used their company accounts for personal communications, and as a result, he believed he could do the same. (*Id.* at p. 241:19-22). Mr. Martland's company Outlook/Exchange account housed his most personal and intimate communications – including emails to his wife (who was his girlfriend at the time time), his mother, and his personal friends. (*Id*. at p. 235:10-18; 307:18-308:13). He coordinated family dinners and trips to see his mother using his company email. (*Id.* at p. 235:10-18). Mr. Martland used his Outlook/Exchange calendar to store his personal appointments such as visits to the doctor's or dentist's office, or dinner with his mother or in-laws. (*Id*. at p. 236:12-22). He also stored his personal contacts in Outlook, which synced with his iPhone. (*Id*. at p. 237:15-238:10). Mr. Martland's Exchange account was password protected with log-in credentials unique to him, and he never shared his credentials with anyone. (*Id*. at p. 224:3-20; p. 239:7-11; p. 242:8-10).

Mr. Martland expected his email communications to remain private, and he did not think anyone at Wellco could access or monitor his emails. (*Id.* at p. 240:9-12). His expectation of privacy was enhanced by the fact that his communications were stored on Wellco's private server, as opposed to being held by a public internet service provider ("ISP") such as Google or Yahoo. (*Id*. at p. 262:13-263:14). Mr. Martland did not receive an employee handbook until a year after he began working at Wellco, and he believed monitoring policies did not apply to him, given the numerous distinctions between associates and managers. (*Id*. at p. 244:17-22; p. 271:14-272:12;

p. 297:9-13; p. 314:7-17). Mr. Martland further believed his Exchange account, along with all of its files, would be shut off and deleted once he left Wellco, and that before leaving he needed to ensure that any relevant documents or emails on his account were forwarded to his administrative assistants. (Tr., p. 288:8-25; p. 318:8-12).

Mr. Martland clearly established that he had a subjective expectation that the government could not obtain his business and personal emails from Wellco's server without a search warrant. *See United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (finding defendant had subjective expectation of privacy business and personal emails stored on a third party public ISP server).

B. Mr. Martland's expectation of privacy was objectively reasonable because any corporate right for Wellco to access or monitor Mr. Martland's emails for business purposes does not equate to *carte blanche* government access.

The Sixth Circuit has recognized that Mr. Martland's expectation of privacy in his business and personal emails – stored on a third-party server with third-party right of access – is objectively reasonable. *See Warshak*, 631 F.3d at 283-88. In *Warshak*, the court examined whether the Stored Communications Act, 18 U.S.C. § 2701, *et. seq*., allowed for the warrantless seizure of over 27,000 of the defendant's personal and business emails from the third-party public ISP's server storing the emails. *United States v. Warshak*, 631 F.3d 266, 283-88 (6th Cir. 2010). The court noted that the fact emails were "stored with, sent or received through, a commercial [ISP]" was a "paramount" consideration", but concluded "it would defy common sense to afford emails lesser Fourth Amendment protection" than is granted to similar forms of communication, such as letters or phone calls. Following this conclusion, the Court held that a search warrant is required to obtain business and personal emails from a third-party server. *Id.* at 286-88 (6th Cir. 2010) (citing *City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008)).

The *Warshak* court rejected the notion that the mere ability of a third-party to access the contents of a communication or even the "right of access" is "sufficient to extinguish a reasonable expectation of privacy" in electronic communications stored on a third-party server. *Id.* at 286-87. The Sixth Circuit noted that the defendant's ISP maintained a policy indicated that "*Nuvox* [the ISP] *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the service." *Warshak*, 631 F.3d at 287. The court stated that this "degree of access granted to NuVox does not diminish the reasonableness of Warshak's trust in the privacy of his emails." *Id*. (generally citing *Katz v. United States*, 389 U.S. 347 (1967)).

Other courts have affirmed this principle. *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 903-08 (9th Cir. 2008) (noting the fact that a service provider may "access the contents of [text] messages for its own purposes is irrelevant" to a user's expectation of privacy because the user "did not expect that the [service provider] would monitor [his] text messages, much less turn over the messages to third parties without [his] consent."), *reversed on other grounds by City of Ontario v. Quon*, 560 U.S. 746, 759-760 (2010); *United States v. Finley*, 477 F.3d 250, 258-59 (5th Cir. 2007) (holding that defendant had standing to challenge the search of text messages and call records on his company-issued cell phone, and the fact that the company could have read defendant's text messages did not diminish his reasonable expectation that he would be "free from intrusion from both the government and the general public."); *United States v. DiTomasso*, 56 F. Supp.3d 584, 596-97 (S.D.N.Y. 2014) (holding that consenting to a chat service's monitoring policy does not mean that a reasonable person would think he was consenting to let the chat service freely monitor his chats if the chat service was working as "an agent of law enforcement."); *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996) ("One always bears the risk that a recipient of an e-mail message will redistribute the e-mail or an employee of the

company will read e-mail against company policy. However, this is not the same as the police commanding an individual to intercept the message.").[2]

Supreme Court authority also acknowledges that a person's reasonable expectation of privacy is not extinguished because materials are held, and can be accessed by, a third party. *See City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2451-2454 (2015) (voiding California law that required owners to disclose guest lists to law enforcement without a warrant); *Riley v. California*, 134 S. Ct. 2437, 2493-94 (2014) (rejecting government's argument that law enforcement should always be able to search a suspected criminal's call logs without a warrant, and holding that a

[2] Numerous other courts have held that individuals have a reasonable expectation of privacy in materials held by a third party, such as text messages, emails, and social media messaging. *See United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (noting that the content of email communications, like letters, deserves Fourth Amendment protections); *United States v. Long*, 64 M.J. 57, 63-65 (C.A.A.F. 2006) (government employee had reasonable expectation of privacy in emails sent through and maintained on government server); *In re Search Warrants for Info Associated with Target Email Accounts/Skype Accounts*, No. 13-MJ-8163-JPO, 2013 U.S. Dist. LEXIS 123129, at *6-12 (D.C. Kan. Aug. 27, 2013) (holding that an individual has a reasonable expectation of privacy in emails stored with, or sent or received through, an electronic communications service provider, and those emails may not be obtained by the government without a search warrant); *R.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F. Supp.2d 1128, 1142 (D.C. Minn. 2012) (comparing social media messaging to emails and holding that an individual had a Fourth Amendment privacy interest in her Facebook messages); *In re United States for an Order Authorizing the Release of Historical Cell-Site Info*, 809 F. Supp.2d 113, 124-26 (E.D.N.Y. Aug. 22, 2011) (holding that individuals have a reasonable expectation of privacy in cell-site-location data despite the fact that the records are collected and stored by a third-party); *Commonwealth v. Fulgiam*, 73 N.E.3d 798, 811-14 (Mass. 2017) (holding that defendant had a reasonable expectation of privacy in the contents of his text messages, and that law enforcement could only obtain the content of the messages from a third-party service provider using a search warrant); *State v. Boyd*, 992 A.2d 1071, 1083 (Conn. 2010) (holding that defendant had a reasonable expectation of privacy in all contents of his cell phone, including his phone number, and the fact that he disclosed his phone number to third parties and did not take steps to keep it confidential did not diminish his expectation that law enforcement could not search his phone without a warrant); *State v. Clampitt*, 364 S.W.3d 605, 607-13 (Mo. App. 2012) (declaring the Stored Communications Act unconstitutional to the extent that it allows law enforcement to obtain an individual's text message communications from service providers without a warrant); *State v. Hinton*. 280 P.3d 476, 483 (Wash. App. 2012) (holding that text messages enjoy Fourth Amendment protections).

search warrant is required to search an individual's cell phone); *Ferguson v. City of Charleston*, 532 U.S. 67, 83 (2001) (recognizing Fourth Amendment reasonable expectation of privacy in medical records held by hospital, even though law enforcement did not obtain records directly from patients, but from third-party hospital instead); *Bond v. United States*, 529 U.S. 334, 338-39 (1999) (holding that placing bag in overhead storage bin did not diminish reasonable expectation of privacy against law enforcement search, even though the bag could be moved or manipulated by the public); *Stoner v. California*, 376 U.S. 483, 489-90 (1969) (holding that hotel guests have a reasonable expectation of privacy against warrantless law enforcement searches in their hotel room, despite the fact that hotel employees have the right to access the room).[3]

The government relies heavily on the privacy and monitoring policies contained in the draft handbooks and documents introduced at the suppression hearing to argue that Mr. Martland could have no reasonable expectation of privacy in his company email account. As an initial matter, the government was unable to prove that the documents represented any final versions of the policies that would have been given to Mr. Martland while he was an employee at Wellco. (*See id*. at p. 109:8-20; p. 183:19-184:7; p. 264:14-265:4).

If the draft policies introduced at the hearing are representative of documents Mr. Martland actually received, his belief that they did not apply to him as a manager-level employee was reasonable. The documents and the policies contained therein are vague and confusing. (*See e.g.*,

[3] *See also* Transcript of Oral Argument, *Carpenter v. United States*, No. 16-402, at p. 23 (Nov. 29, 2017) ("That suggests…that it was never an absolute rule, the third-party doctrine. We limited it when – in *Bond* and *Ferguson* when we said police can't get your medical records without your consent, even though you've disclosed your medical records to doctors at a hospital. They can't touch your bag to feel what's in your bag because an individual may disclose his or her bag to the public.") (Sotomayor, J.) (accessible at https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf (last accessed Dec. 28, 2017))

Exhibit and Witness List [Doc. 135], Exhibit 6, p. 5 (making distinction between manager-level and associate employees); p. 30 (contradictory provisions regarding personal storage of company documents). Further, Mr. Martland observed Lee Ferguson, the CEO of Wellco, disregarding policies about personal use of company email systems, bolstering the reasonableness of Mr. Martland's belief that the policies were inapplicable. (Tr., p. 241:19-22; p. 264:4-13).

Assuming that the policies applied to Mr. Martland, they only create a corporate right of access for *Wellco* to inspect or monitor Mr. Martland's emails for work-related purposes, and in no way diminish Mr. Martland's expectation that his emails would not be disclosed to the *government*. In fact, Wellco employees were specifically told that they were entitled to "safeguards provided by law" in the event of a government investigation. (Exhibit and Witness List [Doc. 135], Exhibit 7, p. 9). Even Agent Witsell acknowledged that a search warrant would be one of the legal safeguards to which Wellco employees were entitled. (*Id*. at p. 103:19-24). Wellco employees had an expectation of privacy that their documents and emails would not be disclosed to the government absent these legal safeguards.

The government has cited *United States v. Roberts*, No. 3:08-CR-175, 2009 U.S. Dist. LEXIS 123188, at *20-21 (E.D. Tenn. Dec. 21, 2009), to argue that Mr. Martland could have no reasonable expectation of privacy in his communications, but the *Roberts* Report and Recommendation supports Mr. Martland's position on all points except for expectation of privacy in business and personal emails, and it is not good authority on that issue following *Warshak*.

Further bolstering the reasonableness of Mr. Martland's expectation of privacy is the fact that, in practice, Wellco's corporate right of access to employee emails was limited and rarely exercised. *See United States v. Long,* 64 M.J. 57, 64 (C.A.A.F. 2006) (holding government employee had objective expectation of privacy in emails stored on government server because the

network administrator testified that policies regarding personal use and monitoring were leniently enforced); *United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir. 2002) (city employee maintained reasonable expectation of privacy in work computer despite network administrator and computer technicians' ability to access it because such access was not routine), *overruled on other grounds by Slanina v. United States*, 123 S. Ct. 69 (2002); *Leventhall v. Knapek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (holding that employee had reasonable expectation of privacy in his workplace computer because employer infrequently exercised its right to access that computer) (cited with approval by *James v. Hampton*, 592 Fed. Appx. 499, 456 (6th Cir. 2015) (finding that employee had reasonable expectation of privacy in her work office)); *see also United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (holding that defendant's objective expectation of privacy was not eliminated by a limited university monitoring policy said that computer inspections would only occur to "protect the integrity of the University and the rights and property of the state.").

No Wellco employee, including Mr. Mason – the senior IT administrator – had physical or virtual access to employee emails. (*Id*. at p. 164:11-13; p. 166:22-167:9). Only one employee's emails were ever monitored by Wellco, and it was for work-related purposes after over a year of serious, persistent job performance issues with that employee, including using email malfunctions as excuses for the failing job performance. (*See generally* Exhibit and Witness List [Doc. 135], Exhibit 12; *see also* Tr., p. 63:24-64:19; p. 197:4-12). Mr. Martland, who managed seven employees, did not even know he could monitor his employee's emails. (*Id.* at p. 241:23-25). There is no question that Mr. Martland's emails were never monitored. (*Id*. at p. 196:25-197:3).

Wellco's monitoring policies were no more invasive than those maintained by the third-party internet service provider in *United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010), and in fact offered greater protection against government intrusion. Mr. Martland's expectation of

privacy was objectively reasonable. Accordingly, Mr. Martland had a subjective and objectively reasonable expectation of privacy in his business and personal emails.

B. As member of upper management at Wellco, Mr. Martland has standing to contest the warrantless seizure of Wellco business documents attributable to him.

"It has long been settled that one has standing to object to a search of his office, as well as of his home." *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968). An employee may have a reasonable expectation of privacy in a business that has been subjected to a search and seizure. *See United States v. Mohney*, 949 F.2d 1397, 1403-1404 (6th Cir. 1991) (citing *Henzel v. United States*, 296 F.2d 650 (5th Cir. 1961). Whether an individual had exclusive control over the seized business records is not determinative of the analysis. *See Mancusi v. DeForte*, 392 U.S. 364, 369-70 (1968); *United States v. Mancini*, 8 F.3d 104 (1st Cir. 1993) (holding mayor had expectation of privacy in his appointment calendar that was accessible by his secretaries and noting that "shared access to a document does not prevent one from claiming Fourth Amendment protection in that document."); *see also United States v. Long*, 64 M.J. 57, 63-65 (C.A.A.F. 2006) (government employee had reasonable expectation of privacy in password-protected emails sent stored on government server).

Relevant to this determination is whether the defendant had a personal connection to the seized business records, whether the defendant took precautions to prevent unauthorized disclosures of such materials, and whether the defendant was one of the targets of the search of the corporation. *See United States v. Nagle*, 803 F.3d 167, 177 (3d Cir. 2015) (citing *Mohney*, 949 F.2d at 1399, 1403); *United States v. SDI Future Health Inc.*, 568 F.3d 684, 691-94 (9th Cir. 2009); *United States v. King*, 227 F.3d 732, 744 (6th Cir. 2001). The fact that an employee had a private office or password protected computer also weighs in favor of a reasonable expectation of privacy in any business documents seized from those locations. *See United States v. Roberts*, No. 3:08-

CR-175, 2009 U.S. Dist. LEXIS 123188, at *17-19 (E.D. Tenn. Dec. 21, 2009); *see also United States v. Ziegler*, 474 F.3d 1184, 1188-92 (9th Cir. 2007) (finding that a private office and password protected computer gave rise to Fourth Amendment protections).

Mr. Martland held an upper management role with Wellco as the Director of Distribution and Logistics. He managed seven employees and reported directly to Lee Ferguson. (Tr., at p. 234:4-7; p. 240:19-23). Mr. Martland had a private office and took steps to protect the business documents he created, including maintaining unique log-in credentials for his workplace computer, domain server, and company email account. (*Id*. at p. 234:16-235:1; p. 239:11). Mr. Martland could store his business files locally on his computer, where they could only be accessed using his unique log-in credentials, or he could store them on the file server maintained on Wellco's private network. (*Id*. at p. 152:3-17). Mr. Martland was the target of the government's search of Wellco. In August 2013, Agent Witsell specifically sought Mr. Martland's documents and emails during his investigation. (*See* Exhibit and Witness List [Doc. 135], Exhibit 2, p. 2).

As a high-level manager at Wellco, Mr. Martland had a reasonable expectation of privacy in any business records that he created or played a role in creating. All such warrantlessly seized documents the government would seek to introduce against Mr. Martland must be suppressed.

IV. EXCLUSION OF THE WARRANTLESSLY SEIZED ELECTRONIC COMMUNICATIONS IS THE ONLY APPROPRIATE REMEDY.

The government admits that it seized materials from Wellco absent a warrant. (*Id*. at p. 70:24-71:9). The government used a Department of Homeland Security Administrative subpoena for the improper purpose of gathering evidence in a criminal investigation – an abuse of administrative subpoena power. *See United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 317 (1978) (noting administrative subpoenas may not be used by the government to "expand its criminal discovery rights"); *United States v. Phibbs*, 999 F.2d 1053, 1077-78 (6th Cir. 1993) (holding that

a government agency must show full probable cause to use an administrative subpoena to gather evidence for a criminal investigation); *United States v. Will*, 671 F.2d 963, 967 (6th Cir. 1981) ("[I]f the [IRS] summons is being issued in aid of a solely criminal investigation…the summons will not be enforced.") (citing *LaSalle*, 437 U.S. at 318); *see also United States v. Lawson*, 502 F. Supp. 158, 165 (D.C. Md. 1980) (holding that DEA administrative warrant used to gather evidence for criminal prosecution violated the Fourth Amendment).

Agent Witsell testified that he was in regular contact with the U.S. Attorney's Office for the Eastern District of Tennessee and that he was conducting a criminal investigation when he issued the administrative summons. (*See* Exhibit and Witness List [Doc. 135], Exhibit 13, p. 2; Tr., p. 73:13-75:3; p. 76:3-8; p. 9:22-10:25). This improper use of an administrative summons enabled the government to bypass judicial review and probable cause requirements to warrantlessly obtain a vast amount of constitutionally protected information.

The government's additional warrantless seizures in 2015 and 2017 were the product of, and influenced by, the governments' initial illegal search and seizure. Agent Witsell testified that the customs summons required Wellco's compliance. (*See* Tr. p. 76:24-77:5; Exhibit and Witness List [Doc. 135], Exhibit 1, p. 1). Mr. Mason, who was involved with each of the government's seizures, testified he understood that on each occasion he provided documents to the government, he was assisting the company in complying with some kind of legal directive. (*Id*. at p. 212:6-17).

The taint of the initial illegal search and seizure from Wellco followed the subsequent document productions by Original Footwear. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 233 (1973) (noting that consent given in response to a claim of lawful authority is not valid); *United States v. Beauchamp*, 659 F.3d 560, 572 (6th Cir. 2011) ("[A] suspect's knowledge of an illegal search can also give rise to a sense of futility."); *see, e.g., Missouri v. Seibert*, 542 U.S. 600, 615-

17 (2004) (holding that once statements are illegally obtained in violation of *Miranda*, subsequent *Miranda* warnings do not cure the coercive effect of the first violation). Law enforcement disregarded the warrant requirement and improperly obtained vast amounts of information from Wellco and, later, its successor company, Original Footwear, under the guise of continued cooperation with the government's investigation that started via an improper administrative demand requiring production of evidence for use in a criminal investigation. Exclusion is the appropriate remedy.

IV. CONCLUSION

For these, and other reasons articulated in Mr. Martland's prior filings, Mr. Martland's warrantlessly seized business documents and electronic communications must be suppressed.

Respectfully submitted this 5th day of January, 2018, by:

STEPHEN ROSS JOHNSON [BPR #022140]
WADE V. DAVIES [BPR # 016052]
Ritchie, Dillard, Davies & Johnson, P.C.
606 W. Main Street, Suite 300
Knoxville, TN 37902
(865) 637-0661
johnson@rddjlaw.com
Counsel for Matthew Harrison Martland

CERTIFICATE OF SERVICE

I hereby certify that on January 5, 2018, a copy of the foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic receipt. All other parties will be served by regular U.S. mail. Parties may access this filing through the Court's electronic filing system.

STEPHEN ROSS JOHNSON